

**CLAIMS**

1           1.     A client for connecting a mobile host to a remote network through  
2     an access network with a single user password, where the access network may be  
3     independent of the remote network in terms of no protocol conversation between  
4     authentication servers in the access network and the remote network, respectively,  
5     and a virtual single account (VSA) has been set up for a user to connect to the  
6     access network and then to the remote network, the client comprising machine  
7     readable instructions stored in a memory medium, which when executed by a  
8     processor:

9                     generate a VSA password and decryption key from the single  
10     password received from the user;

11                    decrypt at least one of a local access network authentication  
12     credential and a remote access authentication credential;

13                    initiate a local access network connection; and

14                    initiate a remote network access connection.

1           2.     The client recited in Claim 1, wherein the machine-readable  
2     instructions, which when executed by the processor, initiate a VSA configuration  
3     update process with a VSA server.

1           3.     The client recited in Claim 2, wherein the machine-readable  
2     instructions, which when executed by the processor, initiate the VSA  
3     configuration update process by:

4                    constructing a VSA information update request message;

5                    sending the VSA information update request message to the VSA  
6   server; and  
7                    receiving a VSA information update response message from the  
8   VSA server.

1            4.        The client recited in Claim 3, wherein the step of decrypting the  
2   remote network authentication credential prior to initiating the remote network  
3   access connection is authorized by an instruction for the mobile host in the VSA  
4   information update request message.

1            5.        The client recited in Claim 1, wherein the machine-readable  
2   instructions, which when executed by the processor, select a local access network  
3   from a current VSA access record stored in the memory medium.

1            6.        The client recited in Claim 1, wherein the machine-readable  
2   instructions, which when executed by the processor, generate the decryption key  
3   in response to a random sequence received from the user.

1            7.        The client recited in Claim 1, wherein the machine-readable  
2   instructions, which when executed by the processor, generate the VSA password  
3   using the expression: VSA password = hash(VSA username || common password  
4   || VSA server || remote network ID), wherein the VSA username identifies the user  
5   to a VSA server, the common password is the single password from the user, and  
6   the remote network ID identifies the remote network serving as a home network  
7   for the mobile host.

1            8.        The client recited in Claim 3, wherein the machine-readable  
2   instructions, which when executed by the processor, generate the VSA update

3 request message “Q” from the expression:  $Q = \text{VSA username} \parallel X \parallel E_{K1}$   
 4 (Synchronization time  $\parallel$  Request content), where X is a random sequence; and K1  
 5 is an encryption key calculated from hash (hash (VSA password)  $\parallel$  X).

1           9.       The client recited in Claim 8, wherein the machine-readable  
 2 instructions, which when executed by the processor, are responsive to the VSA  
 3 information update response message “A” derived from the expression:  $A =$   
 4 Response Code  $\parallel Y \parallel E_{K2}$  (Synchronization time  $\parallel$  Response content), wherein Y  
 5 is a random sequence, and K2 is an encryption key calculated from hash (hash  
 6 (VSA password)  $\parallel Y$ ).

1           10.     The client recited in Claim 1, wherein the machine-readable  
 2 instructions, which when executed by the processor, select local access parameters  
 3 and remote access parameters from a VSA access record stored in the memory  
 4 medium.

1           11.     A system for connecting a mobile host to a remote network  
 2 through an access network with a single password, where the access network may  
 3 be independent of the remote network in terms of no protocol conversation  
 4 between authentication servers in the access network and the remote network,  
 5 respectively, and a virtual single account (VSA) has been set up for a user to  
 6 connect to the access network and then to the remote network, comprising:

7           a VSA server deployed in the remote network, the VSA server including  
 8 machine readable instructions stored in a memory medium, which when executed  
 9 by a processor:

10           send a VSA information update response message to the mobile host in  
11   response to receiving a VSA information update request message from the mobile  
12   host;  
13           verify an authentication credential for the remote network received from  
14   the mobile host; and  
15           authorize a remote gateway in the remote network to connect the mobile  
16   host to the remote network.

1           12.    The system recited in Claim 11, wherein the VSA server includes  
2   machine readable instructions stored in the memory medium, which when  
3   executed by the processor generate the VSA information update response message  
4   “A” from the expression:  $A = \text{Response Code} \parallel Y \parallel E_{K2}(\text{Synchronization time} \parallel$   
5   Response content), wherein Y is a random sequence, and K2 is an encryption key  
6   calculated from hash (hash (VSA password)  $\parallel Y$ ), in response to the VSA  
7   information update request message “Q” from the expression:  $Q = \text{VSA}$   
8   username  $\parallel X \parallel E_{K1}(\text{Synchronization time} \parallel \text{Request content})$ , where X is a  
9   random sequence; and K1 is an encryption key calculated from hash (hash (VSA  
10   password)  $\parallel X$ ).

1           13.    The system recited in Claim 11, wherein the VSA server contains a  
2   plurality of VSA management records, each management record including a  
3   user’s VSA authentication credential.

1           14.    The system recited in Claim 11, wherein the VSA server maintains  
2   access information for at least one local access network and at least one remote  
3   network.

- 1           15.     The system recited in Claim 14, wherein the access information  
2     includes client information for mobile hosts, and management information for at  
3     least one additional VSA server.